The g-Circulant Solutions of $A^m = \lambda J$

S. L. Ma
Department of Mathematical Studies
Hong Kong Polytechnic
Hung Hom, Hong Kong

and

William C. Waterhouse*
Department of Mathematics
Pennsylvania State University
University Park, Pennsylvania 16802

Submitted by Hans Schneider

ABSTRACT

We find a general criterion for an n by n integral g-circulant matrix to have all entries in its mth power equal. We show that the row sum for such a matrix is always divisible by a certain explicit function of n, g, and m, and we construct a new type of $(0,1)$ matrix that satisfies the condition and has exactly this minimum sum. We show in fact that for suitable g we get in this way the minimum for all $(0,1)$ matrices. We also apply this result to find a smallest possible subset of integers modulo n on which a linear function $ax + by$ takes on all values equally often.

INTRODUCTION

Let $c_0, c_1, \ldots, c_{n-1}$ be integers. Let g be an integer, $1 \leqslant g \leqslant n$, and let A be the $n \times n$ "g-circulant" matrix with first row given by the c_j. Several papers [3, 6, 8–10], partly prompted by applications to digraphs, have studied conditions that force some power A^m to have all its entries equal (in symbols, $A^m = \lambda J$). In this paper, we shall derive necessary and sufficient

*Work supported in part by the U.S. National Science Foundation, Grant DMS 8400649.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/87/$3.50

conditions in general. The results will be new even for $(0,1)$ matrices and will include the construction of new examples of such matrices. We shall also show that our examples give matrices minimal among all solutions of $A^m = \lambda J$, circulants or not.

We begin by reviewing the known results. One defines the *Hall polynomial* $f(X)$ for A to be $\sum c_i X^i$. As was pointed out by Lam [8], we have $A^m = \lambda J$ if and only if

$$f(X)f(X^g)f(X^{g^2})\cdots f(X^{g^{m-1}}) \equiv \lambda(1 + X + \cdots + X^{n-1}) \bmod X^n - 1.$$

The value of λ is determined by putting $X = 1$, where we get $(\sum c_i)^m = n\lambda$. Some such λ exists iff the product on the left is divisible by $1 + X + \cdots + X^{n-1}$. This polynomial has no multiple roots, and its roots are the $\zeta \neq 1$ satisfying $\zeta^n = 1$. Hence in terms of the Hall polynomial we have the following criterion [6, 9]:

THEOREM (*). *The g-circulant matrix A has all entries of A^m equal iff every nontrivial nth root of 1 is a root of*

$$f(X)f(X^g)\cdots f(X^{g^{m-1}}).$$

Only a few consequences have been deduced from this result, all involving special relations of g and m (see Corollaries 1.3 and 1.5 below). For general g, nothing is on record except when the first row has the form

$$(1,1,\ldots,1,0,0,\ldots,0).$$

A paper by Wang [10] is devoted to proving that such a row gives a solution when the number of entries equal to 1 is a multiple of $n(n,g)/(n,g^m)$. A paper by King and Wang [3] just recently showed that this condition on the entries is also necessary.

This and all other known results will follow easily from our general theorems. In addition, for each g, m, and n, we shall explicitly construct a $(0,1)$ solution with the smallest possible number of nonzero entries. For some g, this number will be much smaller than we would find by looking only at solutions of the form $(1,\ldots,1,0,\ldots,0)$, and for suitable g it will in fact be minimal even among $(0,1)$ matrices that are not circulants.

1. THE BASIC CRITERION

Let $\mathscr{D}$ denote the set of positive divisors of n, including 1 and n. Define an operation $T: \mathscr{D} \to \mathscr{D}$ by $T(d) = d/(d, g)$, where (d, g) denotes the greatest common divisor of d and g. Note that $T^k(d) = d/(d, g^k)$. If we let $\mathscr{D}[p]$ denote the powers of p in $\mathscr{D}$, then $\mathscr{D} = \prod_{p|n} \mathscr{D}[p]$, and the T-operation is performed on each component separately. Let $h_d(X)$ be the cyclotomic polynomial, the monic polynomial whose roots are the primitive dth roots of 1.

THEOREM 1.1. *Let $c_0, \ldots, c_{n-1}$ be rational numbers with $\sum c_i \neq 0$. Let $\mathscr{D}_0$ be the collection of $d \neq 1$ in $\mathscr{D}$ with $h_d(X)$ dividing $\sum c_i X^i$. Let A be the g-circulant formed from the c_i. Then A^m has all entries equal iff for each $d \neq 1$ in $\mathscr{D}$ there is some $0 \leqslant k \leqslant m-1$ with $T^k(d)$ in $\mathscr{D}_0$.*

Proof. We know by Theorem (*) that A^m will have all entries equal when every nontrivial nth root of unity ζ is a root of

$$f(X) f(X^g) \cdots f(X^{g^{m-1}}).$$

In other words, each ζ should have some power ζ^{g^k} (with $0 \leqslant k \leqslant m-1$) that is a root of $f(X)$. The order of ζ can be an arbitrary $d \neq 1$ in $\mathscr{D}$, and it is easy to see then that the order of ζ^{g^k} is $d/(d, g^k) = T^k(d)$. Thus a root of unity of some one of these orders $T^k(d)$ is a root of f. But f has rational coefficients, and it is well known that each cyclotomic polynomial is irreducible over the rationals. Hence some one of these $T^k(d)$ must be in $\mathscr{D}_0$. ∎

COROLLARY 1.2. *Let A_1 be the g_1-circulant formed from the same initial row as A. Suppose $(n, g) = (n, g_1)$. Then $A^m = \lambda J$ iff $A_1^m = \lambda J$.*

Proof. Since every element d of $\mathscr{D}$ divides n, we have $(d, g) = (d, (g, n))$, and thus the definition of T depends only on (g, n). Hence the criterion in Theorem 1.1 will be the same for g_1 as for g. ∎

COROLLARY 1.3 (Wang [9]; cf. [6], [2]). *If $(g, n) = 1$, then A^m has all entries equal only in the trivial case where all c_i are equal.*

Proof. Here T is the identity, so all $d \neq 1$ must be in $\mathscr{D}_0$. Hence $f(X)$ must be divisible by $\prod h_d(X) = 1 + X + \cdots + X^{n-1}$; and since f has degree $n-1$, it must be a constant multiple of $1 + X + \cdots + X^{n-1}$. ∎

A similar argument shows:

COROLLARY 1.4. *Whenever* $A^m = \lambda J$, *then* $f(X)$ *is divisible by* $1 + X + \cdots + X^{(g,n)-1}$.

COROLLARY 1.5. *If* n *divides* g^m, *then* A^m *has all entries equal if and only if* $f(X)$ *is divisible by* $1 + X + \cdots + X^{(g,n)-1}$.

Proof. Necessity follows from the previous corollary. The condition is sufficient here because if we take $\mathscr{D}_0$ to be any set including the divisors of (g, n), the hypothesis on g guarantees that every larger d will have some $T^k(d)$ in $\mathscr{D}_0$. ∎

In different form, this is the main theorem of [9].

COROLLARY 1.6 (Wang and King [10, 3]). *Let* A *be the* g*-circulant matrix with first row* $(1,1,\ldots,1,0,0,\ldots,0)$, *where there are* e *initial nonzero entries. Then* A^m *has all entries equal if and only if* e *is a multiple of* $n(n,g)/(n,g^m)$.

Proof. Familiar computations with sums of roots of unity show that here $\mathscr{D}_0$ consists of the divisors of e other than 1. We need to determine when every $d > 1$ dividing n has some $T^k(d)$ in $\mathscr{D}_0$ (with $k < m$). We saw in Corollary 1.4 that all divisors of (g, n) must be in $\mathscr{D}_0$, and hence (g, n) must divide e. We must also have some $T^k(n)$ in $\mathscr{D}_0$. But if any $T^k(n)$ divides e, then $T^{m-1}(n)$ will divide e, and so $T^{m-1}(n) = n/(n, g^{m-1})$ must divide e. It is easy to verify that the least common multiple of (g, n) and $n/(n, g^{m-1})$ is $n(n, g)/(n, g^m)$, and thus e must be a multiple of this number.

Conversely, $T^k(d)$ always divides $T^k(n)$ when d divides n, and hence under our condition on e we have $T^{m-1}(d)$ dividing e. If $T^{m-1}(d)$ is not equal to 1, then it is in $\mathscr{D}_0$. If it is equal to 1, look back at the first k with $T^k(d) = 1$; we have then $T^{k-1}(d)$ among the divisors of (g, n), and our condition on e guarantees that these are in $\mathscr{D}_0$. ∎

Finally, we should look briefly at the situation where $\sum c_i = 0$. In this case, of course, $A^m = \lambda J$ forces $\lambda = 0$, since $(\sum c_i)^m = \lambda n$. Thus we are considering the nilpotence of such a circulant. The argument runs exactly like that in Theorem 1.1, except that now 1 is a root of $f(X)$. Here is the conclusion:

THEOREM 1.7. *Let* $c_0, \ldots, c_{n-1}$ *be rational numbers with* $\sum c_i = 0$. *Let* $\mathscr{D}_1$ *be the set of all* d *dividing* n (*including* $d = 1$) *for which* $h_d(X)$ *divides*

$\sum c_i X^i$. *Let A be the g-circulant formed from the c_i. Then A^m is zero iff for each d dividing n there is some $0 \leqslant k \leqslant m-1$ with $T^k(d)$ in $\mathscr{D}_0$.* ■

2. DIVISIBILITY RESTRICTIONS ON $\sum c_i$

How many nonzero c_i do we need in an n by n $(0,1)$ g-circulant A if we want A^m to have all entries equal? At one extreme, of course, it is possible to take all c_i to be 1, so there is always at least one nonzero choice. There is a lower bound independent of g coming from the relation $(\sum c_i)^m = \lambda n$, but this can be attained only for certain g (see the next section). We know that for rows of the form $(1, \ldots, 1, 0, \ldots, 0)$ the least possible sum is $n(n, g)/(n, g^m)$, but it is not hard to find examples with fewer nonzero entries. In this section we shall determine the precise minimum and construct explicitly an example where that minimum is attained; this construction will introduce new examples of some interest. We shall actually show that our minimum value divides $\sum c_i$ for any integral row c_i that makes A^m have all entries equal, and thereby we shall determine the possible λ occurring in solutions of $A^m = \lambda J$ for integral A. We may as well begin by defining the number that will work.

DEFINITION. Write $n = uw$, where w is relatively prime to g and u involves only primes dividing g. Let

$$R = R(n, g, m) = w \prod_{t \geqslant 0} \frac{(n, g^{mt+1})}{(n, g^{mt})}.$$

The product here is finite, since there are no contributions to it once mt exceeds the highest exponent occurring for any prime in n. More precisely, we can see that if $p^b \| n$ and $p^c \| g$ (where we use $\|$ to denote precise divisibility), then each factor in the product contributes a power p^c until we reach the one where $(mt+1)e \geqslant b$, where there may or may not be a contribution. Checking the details in this analysis, one can easily prove the following formula, which gives a prime-by-prime evaluation of R:

LEMMA 2.1. *Let p be a prime dividing n, with $p^b \| n$ and $p^c \| g$. Write $b = cme + ve + s$ with $0 \leqslant v < m$ and $0 \leqslant s < e$ (put $v = 0$, $s = b$ if $e = 0$). Let $r = (c+1)e$ unless $v = 0$, in which case $r = ce + s$. Then $p^r \| R$.* ■

If n divides g^m, we get $R(n, g, m) = (n, g)$, as expected from Corollary 1.5; when n is relatively prime to g, we get $R(n, g, m) = n$. For a more illuminating example, let $n = 2^6 \times 3 = 192$, with $g = 2$, $m = 2$; here $R(192, 2, 2) = 24$.

THEOREM 2.2.

(a) *Let A be an $n \times n$ g-circulant matrix with integer entries. Suppose $A^m = \lambda J$. Then the row sum in A is divisible by $R = R(n, g, m)$.*

(b) *Such an A exists with all entries equal to 0 or 1 and exactly R entries in each row equal to 1.*

Proof. (a): We may assume $\lambda \neq 0$, as otherwise the row sum is 0. Take the set $\mathscr{D}_0$ associated with A. Let p be some prime dividing n, and use the notation of Lemma 2.1. As T preserves $\mathscr{D}[p]$, each p^y with $1 \leqslant y \leqslant b$ has some $T^k(p^y)$ in $\mathscr{D}_0 \cap \mathscr{D}[p]$. As $T(p^y) = p^{y-e}$, the operations T^k preserve congruence classes modulo e in the exponent. There will be exactly s such classes containing $cm + v + 1$ elements each, and $e - s$ classes containing $cm + v$ elements each. There must be at least $1/m$ of each class in $\mathscr{D}_0$. Adding up those numbers, we find that $\mathscr{D}_0 \cap \mathscr{D}[p]$ contains at least $e(c + 1)$ elements if $v > 0$ and at least $ec + s$ elements if $v = 0$. Thus $|\mathscr{D}_0 \cap \mathscr{D}[p]| \geqslant r$.

Now every p^y occurring in $\mathscr{D}_0 \cap \mathscr{D}[p]$ corresponds to a factor

$$\frac{1 - X^{p^y}}{1 - X^{p^{y-1}}} = 1 + X^{p^{y-1}} + X^{p^{y-1}(p-1)} + \cdots + X^{p^{y-1}(p-1)}$$

dividing $\sum c_i X^i$. As these factors are primitive, the quotient has integral coefficients. Setting $X = 1$, we see that $\sum c_i$ is divisible by p^r.

(b): To construct the example, we use the original definition of R. We know from Theorem 1.1 that we want a polynomial $f(X) = \sum c_i X^i$ that has $(0, 1)$ coefficients and an appropriate set $\mathscr{D}_0$. We start by specifying $\mathscr{D}_0$: it is to be the divisors of w (other than 1) together with, for all t, the divisors of $w(n, g^{mt-1})$ that do not divide $w(n, g^{mt})$. It is easy to check that this set satisfies the requirement of Theorem 1.1. The product of the cyclotomic polynomials for this set of divisors comes out to be

$$\frac{X^w - 1}{X - 1} \prod \frac{X^{w(n, g^{mt-1})} - 1}{X^{w(n, g^{mt})} - 1}$$

A typical factor here, when expanded, gives

$$1 + X^{w(n,g^{m'})} + X^{2w(n,g^{m'})} + \cdots + X^{w(n,g^{m'-1})\cdot w(n,g^{m'})}.$$

Hence the gaps occurring between the exponents in each factor are greater than the sum of the highest exponents occurring in the previous factors, and the polynomial has only 0 and 1 as coefficients. The total number of terms occurring is obviously R. ∎

The construction here can be varied to give other examples of $(0,1)$ circulants with $A^m = \lambda J$.

As an example, we noted earlier that $R(192,2,2) = 24$, and thus the theorem tells us how to find a 192×192 2-circulant matrix A with all entries in A^2 equal and just 24 entries equal to 1. If we had restricted ourselves to 2-circulants with initial rows of the form $(1,\ldots,1,0,\ldots,0)$, Corollary 1.6 shows that we would need 96 initial 1's.

COROLLARY 2.3. *Let n, g, m, and λ be integers. There is an integral $n \times n$ g-circulant matrix A with $A^m = \lambda J$ iff λ/n is the nth power of a multiple of $R(n,g,m)$.*

Proof. We know $n\lambda = (\sum c_i)^n$, and thus the condition is clearly necessary; and if the condition is satisfied, we can take A to be an integer multiple of the minimal $(0,1)$ example. ∎

3. MINIMAL (0,1) MATRICES WITH $A^m = \lambda J$

We can now show that the g-circulant matrices we have been studying actually include solutions to our equation that are minimal among all matrices. If $n = \prod p^{b(p)}$, let $g_0 = \prod p$, and let R denote $R(n, g_0, m)$, so that $R = \prod p^{r(p)}$ with $r(p) =$ the least integer $\geqslant b(p)/m$.

THEOREM 3.1.

(a) *Let A be* any *$n \times n$ integral matrix for which $A^m = \lambda J$. Then the rows of A have sum divisible by R (and hence $n\lambda$ is an nth power of a multiple of R).*

(b) *There is a g_0-circulant $(0,1)$ matrix that satisfies $A^m = \lambda J$ and has row sum precisely R (and hence $n\lambda = R^m$).*

Proof. Statement (b) follows from Theorem 2.2; we must prove (a). It is well known that A must have all row sums (and column sums) equal to some one number s, and that $s^m = n\lambda$ (see for instance Lam [8, Theorem 4.1]). As the entries in A are integers, λ is an integer, and thus n divides s^m. Hence each prime p dividing n must divide s. More precisely, if $p^b \| n$ and $p^h \| s$, then we must have $mh \geqslant b$; that is, $h \geqslant b/m$. Thus R divides s. ∎

COROLLARY 3.2. *There is a nontrivial $n \times n$ $(0,1)$ matrix A with A^m having all entries equal if and only if n is divisible by the square of some prime. When one exists, it can be chosen to be a g_0-circulant.*

Proof. If n is square-free, we have $R = n$, and no nontrivial solution is possible. In all other cases, $R < n$. ∎

This strengthens a theorem of King and Wang [3, Theorem 5.1].

COROLLARY 3.3. *There is a nontrivial $(0,1)$-matrix satisfying $A^m = J$ iff n is an mth power, and in that case we can find an example which is a g_0-circulant.* ∎

4. APPLICATION TO FUNCTIONS REPEATING ALL VALUES EQUALLY OFTEN

PROPOSITION 4.1. *Let S be a nonempty subset of $\mathbb{Z}/n\mathbb{Z}$, with $|S| = s$. Suppose that the s^2 sums $x + gy$ (for x and y in S) represent every value modulo n (including 0) the same number of times. Then the cardinality s is divisible by $R = R(n, g, 2)$, and an example exists with $s = R$.*

Proof. Let A be the $(0,1)$ g-circulant with $c_i = 1$ iff i is in S. As was noted by Lam [6], the condition on S is equivalent to requiring that A^2 have all its entries equal. The proposition thus follows from Theorem 2.2. ∎

Observe that the proof of Theorem 2.2 actually gives an explicit example. For instance, let us take $n = 192$ and $g = 2$. The polynomial constructed there for $m = 2$ is

$$(1 + X + X^2)(1 + X^3)(1 + X^{15})(1 + X^{96}).$$

To find S, we simply expand out this product and take the exponents of the

terms occurring, and we get

$$S = \{0,1,2,3,4,5,24,25,26,27,28,29,96,97,98,$$

$$99,100,101,120,121,122,123,124,125\}.$$

The function $x+2y$ for x and y in this set yields every value modulo 192 exactly 3 times.

For our last theorem, we will need a slight generalization of this result, allowing the values for x and y to occur repeatedly; the proof is still the same. The statement is this:

LEMMA 4.2. *Suppose we allow x and y to take on values* mod n *(independently), and the value i is taken on c_i times. Suppose $x+gy$ takes on all values* mod n *equally often. Then $\sum c_i$ is divisible by $R(n,g,2)$.*

This allows us to extend Proposition 4.1 from the function $x+gy$ to a general linear function.

THEOREM 4.3. *Let S be a nonempty subset of $\mathbb{Z}/n\mathbb{Z}$ with $|S| = s$. Suppose that the s^2 values $gx+hy$ (for x and y in S) represent every value modulo n the same number of times. Then:*

(1) *No prime divides all three of n, g, and h.*

(2) *Write $n = n_1 n_2$ with $(n_1, n_2) = (n_1, g) = (n_2, h) = 1$. Then the cardinality s is divisible by $R_1 R_2 = R(n_1, h, 2)R(n_2, g, 2)$.*

(3) *An example can be constructed with $s = R_1 R_2$.*

Proof. Obviously no prime can divide n, g, and h, since then only values containing that prime could occur. Hence we can indeed decompose n as in (2), including all primes dividing h in n_1 and all primes dividing g in n_2. This decomposition may not be unique, since prime factors of n not involved in either g or h can be put in either n_1 or n_2. But those factors then simply occur unchanged as factors in $R(n_1, h, 2)$ and in $R(n_2, g, 2)$, so the product $R_1 R_2$ is always the same no matter which decomposition is chosen.

We can now construct the example in (3). Choose a number b so that $bg \equiv 1 \bmod n_1$. Since b is relatively prime to n_1, we have $R_1 = R(n_1, h, 2) = R(n_1, bh, 2)$. Choose then a subset S_1 of numbers modulo n_1 that contains R_1 elements and for which $x + bhy$ takes on all values modulo n_1 equally often. As g is relatively prime to n_1, it follows that $gx + hy$ (which is congruent to $gx + gbhy$) also takes on all values modulo n_1 equally often on S_1. In exactly the same manner, we can find a subset S_2 of numbers modulo n_2 that

contains R_2 elements and for which $gx + hy$ takes on all values modulo n_2 equally often. By the Chinese remainder theorem, we can pair all elements in S_1 with all elements in S_2, getting a subset S of numbers modulo n; this subset will contain R_1R_2 elements, and $gx + hy$ on that set will take on all values modulo n equally often.

Finally, we must show that this cardinality divides the cardinality of every other possible subset S. As R_1 involves only primes dividing n_1, and similarly for R_2, the two are relatively prime; hence it will suffice to show that each of these R_i divides $|S|$. We write out the argument for R_1. For each class i modulo n_1, let c_i be the number of elements in S that are congruent to i modulo n_1. Taking x and y modulo n_1 (with the value i repeated c_i times), we see that $gx + hy$ takes on all values modulo n_1 equally often. Multiplying by b as in the previous paragraph, we see that $x + bhy$ takes on all values modulo n_1 equally often. By Lemma 4.2, we can conclude that $R(n_1, bh, 2)$ [which is the same as R_1] must divide Σc_i [which is the same as $|S|$]. ■

As in Proposition 4.1, we should note that we have an explicit process for constructing a minimal S.

REFERENCES

1 C. M. Ablow and J. L. Brenner, Roots and canonical forms for circulant matrices, *Trans. Amer. Math. Soc.* 107:360–376 (1963).

2 W. G. Bridges and R. A. Mena, X^k-Digraphs, *J. Combin. Theory Ser. B* 30:136–143 (1981).

3 F. King and K. Wang, On the g-circulant solutions to the matrix equation $A^m = \lambda J$, II, *J. Combin. Theory Ser. A* 38:182–186 (1985).

4 C. W. H. Lam, A generalization of cyclic difference sets I, *J. Combin. Theory Ser. A* 19:51–65 (1975).

5 C. W. H. Lam, A generalization of cyclic difference sets II, *J. Combin. Theory Ser. A* 19:177–191 (1975).

6 C. W. H. Lam, On rational circulants satisfying $A^2 = dI + \lambda J$, *Linear Algebra Appl.* 12:139–150 (1975).

7 C. W. H. Lam, Cyclotomy and addition sets, *J. Combin. Theory Ser. A* 22:43–60 (1977).

8 C. W. H. Lam, On some solutions of $A^k = dI + \lambda J$, *J. Combin. Theory Ser. A* 23:140–147 (1977).

9 K. Wang, On the matrix equation $A^m = \lambda J$, *J. Combin. Theory Ser. A* 29:134–141 (1980).

10 K. Wang, On the g-circulant solutions to the matrix equation $A^m = \lambda J$, *J. Combin. Theory Ser. A* 33:287–296 (1982).

Received 4 February 1985; revised 18 December 1985